National Security Agency/Central Support Service

INFORMATION ASSURANCE DIRECTORATE

CGS Network Mapping Capability

Version 1.1.1

The Network Mapping Capability helps visualize the network and understand relationships and connectivity between all devices and the communications that provide service. Network Mapping is conducting Enterprise-level mapping of all network components. This mapping should depict every network component's network connectivity, at the nodal, logical, and physical level.

07/30/2012

Table of Contents

CGS Network Mapping Capability
Version 1.1.1

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2   Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

The Network Mapping Capability helps visualize the network and understand relationships and connectivity between all devices and the communications that provide service. Network Mapping is conducting Enterprise-level mapping of all network components. This mapping should depict every network component's network connectivity, at the nodal, logical, and physical level.

For this Capability, network components shall be defined as every network device connected to the network, whether it has an Internet Protocol (IP) address and whether it is physically connected (shall also include wireless devices).

3   Capability Gold Standard Guidance

The CGS for IA provides comprehensive, measurable, IA guidance for securing NSS Enterprises while enabling the mission in the face of continuous attack. CGS defines what it means for Capabilities to be considered "gold." That is, it characterizes the highest level of practice for IA Capabilities in accordance with policies, standards, and best practices, while considering the limitations set forth by current technologies and other constraints.

The Enterprise shall be able to identify its network components. Network Mapping provides a visual device-level interpretation that captures all nodes on a network. Different levels of detail need to be represented at various Enterprise levels. For example, the Enterprise-level (Organization with defined mission/ goal and defined boundary) mapping may need a different picture or include different information (perhaps at a higher level) than a department-level mapping, and the department-level different from enclave-level (collection of systems under the control of a single authority), etc. All mappings shall have a searchable function or the potential to run ad hoc queries to locate devices.

Implementation of the Network Mapping Capability shall include the ability to conduct real-time (or near real-time) automated local-level and subsequent Enterprise-level Network Mappings of all network components, where possible. Real-time (or near real-time) may be achievable only for components that are discoverable. Not all network components are "discoverable" by automated means, and Network Mapping may require

some manual input, particularly for physical location. Based on technology today, mapping at the nodal and logical level can be completed by discovery via the communication protocol that the component employs to communicate on the network.

For components that are not discoverable and require manual mapping, date/time stamps are included for the mapping to determine when the last mapping was completed. When examining the value of real-time (or near real-time) mapping, consideration shall also be given to the volatility of the environment for the network components of a particular mapping. If the environment is relatively static, mappings may be updated at a lower frequency. If the environment is more dynamic (mobile devices, temporary installations, etc.), frequency of the mapping shall be completed at a higher rate (to be set by the Enterprise).

This mapping shall depict every network component's connectivity and physical location. It shall also provide a visual representation of the network component type that is interactive (e.g., drill down into network component detail). The level of detail of location information provided by each map shall be related to the intended purpose and users of that map. At this time, Security Content Automation Protocol (SCAP) does make provisions for geographic information to satisfy physical location.

Retention of the mapping data shall be based on frequency of the updates as well as the needs of the users of the maps. Retention of the data shall enable historical creation of the map from a particular point in time.

The format of the network maps shall use an industry- or Community-established standard (when possible) to facilitate integration with various mapping tools and provide accurate graphical representations of the network. The Network Mapping Capability shall also be able to import information from other Capabilities (Configuration Management, Network Enterprise Monitoring, Network Boundary and Interfaces, among others) and be able to display information relevant to the network components. To seamlessly import and export information and function as a standardized and interoperable capability, Network Mapping shall use only standard and secure protocols, where possible, for discovery, processing, and reporting.

4   Environment Pre-Conditions
The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are

services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. Network boundaries are clearly defined.
2. Mapped network components are configured for security (i.e., hardened operating systems and services).
3. The network implements standard network protocols and services.
4. The network may or may not contain virtualized environments.
5. The environment contains Network Operations and Planning Centers for analysis of the Capability output.
6. The appropriate governance structures are in place to allow for the collection and sharing of the Network Mapping data, if needed.
7. Legal issues have been resolved and legal authority has been established with respect to gathering and sharing of Network Mapping data, if needed.
8. Isolated enclaves on the network have the ability to provide Network Mapping information to the Capability.
9. The Organization is in compliance with current Information Assurance (IA) Policies and Procedures.
10. Aggregation of data for classified environments will occur using the appropriate protections or out-of-band (OOB) networks, depending on the Organization's policy.

5   Capability Post-Conditions
The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability is able to map all network components (e.g., for systems that have been hardened).
2. The Capability relies on secure network services to perform its functions.
3. The Capability is able to uniquely identify all physical network components on the network; some virtualized environments may not be able to be mapped.
4. The Capability provides aggregated views of multiple community of interest (COI) networks while still respecting each COI's security needs.
5. The Capability is not responsible for operating system identification, or other such application or service identification.
6. The Capability output is in standard format such that it is exportable to Network Operations and Planning Centers' applications.
7. The Capability is able to identify the physical location of all network devices.

8. The Capability provides the option to import data from other Capabilities that are needed for understanding the network components and links for display.
9. The Capability does not adversely affect normal operations.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

When Network Mapping is employed correctly, the Organization will possess a capability to identify network assets via a real-time (or near real-time) automated Network Mapping. The tool will produce up-to-date network diagrams depicting network components (as defined in the Capability definition), including an interactive visual representation of the network component type and operational status of the component and the related connections.

The Organization will ensure that any tools selected to conduct network mapping functions will employ industry standard formats. In addition, when selecting a tool, consideration will be given to the relationship between the Network Mapping Capability and other Capabilities (see Capability Interrelationships section). Some tools may aid in implementing related Capabilities.

Network Mapping will be conducted in a manner so as not to interrupt mission resources or the required availability of the system. It will be carried out by personnel possessing the necessary system rights and privileges (e.g., system administrators, network administrators). Network maps will not be available to all general users. The network diagrams will be protected at the same or higher classification as the network they are depicting. Network maps will be retained with respect to their use and frequency of their updates.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Network Boundary and Interfaces–The Network Mapping Capability relies on the Network Boundary and Interfaces Capability for information about resources on the network boundaries.
- Configuration Management–The Network Mapping Capability relies on the Configuration Management Capability to ensure that all network boundary devices, entry points, and exits are compliant with configurations as outlined in the Configuration Management Plan.
- Network Enterprise Monitoring–The Network Mapping Capability relies on the Network Enterprise Capability to provide information about network activities, which can include asset locations.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management–The Network Mapping Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards–The Network Mapping Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness–The Network Mapping Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Network Mapping Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Network Mapping Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Utilization and Performance Management–The Network Mapping Capability relies on the Utilization and Performance Management Capability to ensure that mapping activities do not interfere with mission operations.
- Network Security Evaluations–The Network Mapping Capability relies on the Network Security Evaluations Capability for information, which is used to fill any gaps that may have been overlooked by network mapping activities.
- Risk Mitigation–The Network Mapping Capability relies on the Risk Mitigation Capability to select individual countermeasures that may need to be implemented.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
CM-2 *BASELINE CONFIGURATION*	Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. Enhancement/s: (1) The organization reviews and updates the baseline configuration of the information system: (a) [Assignment: organization-defined frequency]; (b) When required due to [Assignment organization-defined circumstances]; and (c) As an integral part of information system component installations and upgrades. (2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.
PL-2 *SYSTEM SECURITY PLAN*	Control: The organization: a. Develops a security plan for the information system that:

- Is consistent with the organization's enterprise architecture;
- Explicitly defines the authorization boundary for the system;
- Describes the operational context of the information system in terms of missions and business processes;
- Provides the security category and impact level of the information system including supporting rationale;
- Describes the operational environment for the information system;
- Describes relationships with or connections to other information systems;
- Provides an overview of the security requirements for the system;
- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Reviews the security plan for the information system [*Assignment: organization-defined frequency*];

Enhancement/s:

(1) The organization:

(a) Develops a security Concept of Operations (CONOPS) for the information system containing, at a minimum: (i) the purpose of the system; (ii) a description of the system architecture; (iii) the security authorization schedule; and (iv) the security categorization and associated factors considered in determining the categorization; and

(b) Reviews and updates the CONOPS [*Assignment: organization-defined frequency*].

Enhancement Supplemental Guidance: The security CONOPS may be included in the security plan for the information system.

(2) The organization develops a functional architecture for the information system that identifies and maintains:

(a) External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface.

9   Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Network Mapping Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Department of Defense Intelligence Information System (DODIIS) IPSONAR Network Mapping Initiative, DIA CIO Policy #01-07, 1 February 2007, Unclassified	Summary: An excerpt from the document: 1. In order to provide an understanding of the expanse of the Joint Worldwide Intelligence Communications System (JWICS) network environment, connections, and architecture, the Defense Intelligence Agency (DIA) was appointed as the Executive Agent for Network Mapping on behalf of the Director National Intelligence (DNI). The Information Protection Center (IAPC) has been appointed as executing authority for this network operation. The IPSONAR sensor and server suite have been implemented to complete this task. 2. The IAPC completed deployment of this capability across the entire domain. Sensors have been deployed in accordance with the JWICS architecture to maximize effectiveness and minimize any network interference.
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	

Other Federal (OMB, NIST, …)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	

Network Mapping Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
Asset Reporting Format (ARF), An Emerging Specification of the NIST Security Content Automation Protocol (SCAP), Unclassified	The Asset Reporting Format (ARF) language is a general security automation results reporting language developed by the DoD in conjunction with the National Institute for Standards and Technology (NIST) and members of the Security Content Automation Protocol (SCAP) vendor community. It provides a structured language for exchanging and exporting detailed, per-device assessment data between network assessment tools.
Executive Branch (EO, PD, NSD, HSPD, …)	

Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, …)	
Nothing found	

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Scope of work–As the size and complexity of the network grows, costs will grow with them. Complexity includes the number and type of network components.
2. Network acquisition requirements–These requirements may affect the ability of devices to respond to mapping techniques and may limit the toolset available to this Capability.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements

that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Network Mapping Capability.

- The Enterprise shall use network mapping to help visualize the network and understand relationships and connectivity between all devices and the communications that provide service. This mapping shall depict every network component's network connectivity, at the nodal, logical, and physical level.
- The Enterprise shall be able to identify its network components.
- All network mappings shall have a searchable function or the potential to run ad hoc queries to locate devices.
- Network mapping, the visual device-level rendering, of all local and Enterprise-level network components shall be automated, where possible.
- Network mapping for components that are discoverable shall be updated in real-time, where possible.
- All network mappings shall have date-time stamps.
- For networks that are more dynamic, (mobile devices, temporary installations, etc.) network maps shall be updated more frequently (to be set by the Organization).
- Network mapping shall depict every network component's connectivity and physical location and provide a visual representation of the network component type that is interactive.
- The level of detail of network systems shall be related to the intended purpose and users of that map.
- Network components shall be mapped to provide connectivity and physical location and provide visual representation of the nodes (end-points, intermediary, switches, etc.).
- The network maps shall use an industry standard format to facilitate integration with various mapping tools and provide accurate graphical representations of the network.
- The network mapping system shall be able to import information from other systems including configuration management, network enterprise monitoring, network boundary and interfaces and be able to display information relevant to the network components.
- Network mapping shall use only standard and secure protocols, where possible, for discovery, processing, and reporting of information.